REMARKS

Claims 1-42 remain in this application. Claims 1 and 22 are amended. Applicants acknowledge with appreciation the withdrawal of the previous grounds of rejection. Applicants respectfully request reconsideration and review of the application in view of the foregoing amendments and following remarks.

Before addressing the merits of the rejections based on prior art, Applicants provide the following brief description of the patent application. The invention provides a form of data encryption/decryption in which the encrypted information can be decrypted only at a specified location. The location information is used to generate the key to encrypt and decrypt the information, referred to herein as a geolocking key. If someone attempts to decrypt the data at another location, the decryption process fails and reveals no details about the original plaintext information. The device performing the decryption determines its location using some sort of location sensor, such as a GPS receiver or other satellite or radio frequency positioning system.

More specifically, the patent application describes the use of a location identity attribute that defines a specific geographic location. The digital information is encrypted and decrypted using a geolocking key based on the location identity attribute. The appliance that receives the encrypted digital information generates the geolocking key to decrypt the digital information based on its knowledge of the physical location of the appliance. Notably, the geolocking key is not communicated to the receiving appliance—to the contrary, it is generated at the receiving end. If the appliance location is not within the proximate area of the location identity attribute, the appliance will be unable to generate the geolocking key to decrypt the digital information. More accurately, it will generate a key that will not be the right one to decrypt the digital information. By allowing decryption of the digital information only at the specific geographic location, the present invention enforces the location identity.

In accordance with certain embodiments of the invention, the location identity attribute further includes a shape parameter that defines a shape of a region that encompasses the specific geographic location in which the information is to be accessed. The shape parameter does not identify the location, so location cannot be discerned from the shape parameter alone. For example, the shape parameter may define the shape of the neighborhood in which the receiver is located, and all receivers in the same neighborhood may utilize the same shape parameter. The shape parameter is used along with the location data to generate the geolocking keys. This way, the shape parameter can be communicated to the receiving appliance along with the encrypted data. The receiving appliance would use the shape parameter along with its knowledge of its own geographic location (e.g., using a GPS receiver) to generate the geolocking key and thereby recover the encrypted information. Since the location data is not communicated, the geolocking key could not be generated by an unauthorized person that intercepts the communication and obtains the shape parameter.

The claims of the present application address both ends of the information communication process, i.e., encrypting (sending) end and decrypting (receiving) end. Independent Claims 1 and 22 each address the encryption of information at the sending end in respective method and apparatus claim forms, and are amended above to clarify certain aspects of the invention. In contrast, independent Claims 14 and 34 each address the decryption of information at the receiving end in respective method and apparatus claim forms. Notably, the decryption claims further include limitations directed to the use of the shape parameter.

The Examiner rejected Claims 1-8, 11, 14-19, 21-29, 32-39, and 41-42 under 35 U.S.C. § 103(a) as unpatentable over Murphy in view of Schipper et al. Applicants respectfully traverse this rejection.

Murphy is directed to the control over decryption of encrypted signals based on the location where the decryption is performed. More particularly, Murphy discloses a decryption module that includes a Satellite Positioning System (SATPS) antenna and signal receiver/processor. The decryption module (1) determines the present location of the antenna, (2) compares the present location with a licensed site location for the particular decryption chip, and (3) shuts down or disables the signal decryption routine if the SATPS-determined present location of the antenna does not match the licensed site location. As shown in Fig. 2, an activation switch 31i is coupled to the decryption chip 15i, and will deactivate the decryption chip if the antenna is determined to not be in the proper location. The encrypted signals (ES) can only be decrypted when the decryption chip is activated.

As discussed in the response to the previous Office Action, there are very significant differences between Murphy and the present invention. First of all, Murphy does not disclose the encryption of data signals. To the contrary, the reference is directed solely to the decryption of encrypted signals. In fact, Murphy includes no discussion of the source of the encrypted signals other than that they are transmitted to the licensed sites by one or more satellites. See col. 7, lns. 23-26. Murphy therefore has no applicability whatsoever to independent Claims 1 or 22, which each address the encryption of information at the sending end of a communication system. The Examiner fails to consider this deficiency of Murphy in the present Office Action.

Second, Murphy does not use location information to generate a decryption key, and does not encrypt or decrypt digital information using a geolocking key based on a location identity attribute. The Examiner has acknowledged these deficiencies of Murphy in the present Office Action, and proposes the combination with Schipper to make up for these deficiencies.

Schipper discloses a method of communicating between mobile stations using present and past location information to vary an encryption key. The mobile stations each have a satellite positioning system (SATPS) receiver and antenna that receive signals from a plurality of navigation satellites. The SATPS receiver generates pseudorange measurements from that station to each navigation satellite in view, and produces location information based on a plurality of pseudorange measurements.

Schipper periodically communicates pseudorange correction values (PRC) from a base station to the mobile stations, which in turn use these pseudorange correction values to correct their own location determinations. By design, Schipper purposefully eliminates location from the correction values by calculating them as the differential between the known base station location and the SATPS pseudorange measurements. The mobile stations also use the pseudorange correction values as a parameter to determine the encryption key for messages transmitted to other mobile stations. The pseudorange correction values can be used as an encryption key because they represent a convenient mathematical value known to each of the mobile stations that changes over time to provide added security.

According to the Examiner, "Schipper discloses an apparatus for location specific encryption and decryption of a signal wherein communications are encrypted or decrypted by a key based on one or more location attributes." This conclusion is not correct. The pseudorange correction values do not uniquely identify a geographic location, but instead represent the difference between the known location of the fixed station and the calculated location. In other words, Schipper starts with an accurate determination of location, and then subtracts out the location calculation to get the pseudorange correction values, which are essentially "noise." Schipper then uses the "noise" as the common encryption key. Moreover, the pseudorange correction values are common to all mobile stations that communicate with the fixed station (see col. 8, lines 23-28), and do not uniquely identify the geographic location of the mobile station. It is therefore erroneous for the Examiner to consider the pseudorange correction values as analogous to a location identity attribute.

Furthermore, the Examiner incorrectly concludes that "Murphy and Schipper are analogous arts in that they both pertain to location-based encryption/decryption." Schipper does not disclose location-based encryption or decryption. There is nothing disclosed in Schipper that limits access to encrypted information at a specific geographic location. Any mobile station located anywhere could access the encrypted communications as long as it has the pseudorange correction values used as an encryption key. Insofar as the Examiner's sole basis asserted for a teaching or suggestion to combine the references is false, Applicants respectfully submit that the proposed combination of references is improper.

Regardless, even if such a teaching or suggestion to combine were present, the proposed combination of references fail to disclose the claims of the present patent application. The pseudorange correction values of Schipper do not define "at least a specific geographic location of at least one intended recipient of the digital information," as defined in Claims 1 and 22, because they constitute information common to all mobile stations in communication with the fixed station no matter where located. Schipper thus fails to make up for deficiency of Murphy described above insofar as the reference fails to suggest or disclose, *inter alia,* the steps of "generating a unique geolocking key based at least in part on said location identity attribute; and ... encrypting said digital information using said geolocking key, wherein said encrypted digital information can be accessed only at said specific geographic location of the at least one recipient," as defined in Claims 1 and 22. In Schipper, the pseudorange correction values are not generated by the receiver—they are sent by the fixed station to the mobile stations. This security risk is avoided in the present invention by having the recipient device generate the geolocking key based on its knowledge of its physical location.

With regard to Claims 14 and 34, and all claims dependent thereon, the Examiner concludes without analysis or support that these claims are "analogous to the claims 1-9 and 11 rejected above, and therefore rejected following the same reasoning." As noted above, Claims 14 and 34 include different limitations than Claims 1 and 22. For example, Claims 14 and 34 further define the step or function of "generating a geolocking key using at least said shape parameter and said location data." Neither Murphy nor Schipper disclose anything corresponding to a "shape parameter" used to generate a geolocking key, and the Examiner fails to identify any teaching or suggestion in either reference for such a "shape parameter."

Accordingly, the Examiner has failed to make a *prima facie* case of obviousness pursuant to 35 U.S.C. § 103(a). These grounds of rejection should therefore be withdrawn.

The Examiner rejected Claims 9-10, 12-13, 20, 30-31, and 40 under 35 U.S.C. § 103(a) as unpatentable over Murphy in view of Schipper et al., and further in view of Shimada. Applicants respectfully traverse this rejection.

Shimada discloses a data processing method in which access to information is controlled using a password and location attribute data. A data file includes fields for the attachment of attributes defining a password and location. When it is desired to access the data file, a data processing system compares the attached password to one inputted by a user, and also compares the attached location data to a current location determined by a location determining system (e.g., GPS). If the password is correct and the location matches, then access to the data file is permitted.

The Examiner incorrectly concludes that Shimada discloses a system in which a "shape file" is included with the file that contains the digital information. The location data of Shimada contains only a descriptor of the location, and does not define "a shape of a region that encompasses said specific geographic location," as defined in Claims 6, 14, 27 and 34 (on which the rejected claims depend). Unlike the location descriptor of Shimada, the "shape parameter" of the invention does not disclose the location, and therefore may be communicated with the digital information without security risk. In fact, none of the references of record disclose or suggest anything analogous to the "shape parameter" defined in the claims. These grounds of rejection should be withdrawn as well.

In view of the foregoing, Applicants respectfully submit that Claims 1-42 are in condition for allowance. Reconsideration and withdrawal of the rejections is respectfully requested, and a timely Notice of Allowability is solicited. If it would be helpful to placing this application in condition for allowance, the Applicants encourage the Examiner to contact the undersigned counsel and conduct a telephonic interview.

While the Applicants believe that no fees are due in connection with the filing of this paper, the Commissioner is authorized to charge any shortage in the fees, including extension of time fees, to Deposit Account No. 50-0639.

Respectfully submitted,

Date: February 24, 2005

Brian M. Berliner
Attorney for Applicants
Registration No. 34,549

O'MELVENY & MYERS LLP
400 South Hope Street
Los Angeles, CA 90071-2899
Telephone: (213) 430-6000